



Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at <http://about.jstor.org/participate-jstor/individuals/early-journal-content>.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

Modular Invariants of Two Pairs of Cogredient Variables.

BY WILLIAM C. KRATHWOHL.

Introduction.

§ 1. By the term invariant will here be understood a polynomial I in x_1, y_1, x_2, y_2 with integral coefficients taken modulo p such that

$$I(x_1, y_1, x_2, y_2) \equiv (ad - bc)^\mu I(x'_1, y'_1, x'_2, y'_2), \quad (\text{mod. } p),$$

for every transformation

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}: \quad \begin{aligned} x_1 &= ax'_1 + by'_1, & x_2 &= ax'_2 + by'_2, \\ y_1 &= cx'_1 + dy'_1, & y_2 &= cx'_2 + dy'_2, \end{aligned}$$

with integral coefficients.

The constant exponent μ is called the *index* of the invariant.

The main result of the investigation is the following

THEOREM. *As a fundamental system of invariants we may take*

$$\begin{aligned} L_i &= \begin{vmatrix} x_i^p & y_i^p \\ x_i & y_i \end{vmatrix}, & Q_i &= \begin{vmatrix} x_i^{p^2} & y_i^{p^2} \\ x_i & y_i \end{vmatrix} / L_i, & (i = 1, 2), \\ M &= x_2 y_1 - y_2 x_1, & M_1 &= x_2 y_1^p - y_2 x_1^p, & M_2 &= x_2^p y_1 - y_2^p x_1, \\ N_s &= \frac{M_2^{s+1} L_1^{p-s-1} + (-1)^s M_1^{p-s} L_2^s}{M^p}, & (1 \leq s \leq p-2). \end{aligned}$$

The absolute invariants Q_i^* and N_s are actually integral functions of x_1, y_1, x_2, y_2 .

Among the syzygies needed are

$$\begin{aligned} (S_0) \quad L_1 L_2 + M_1 M_2 - M^{p+1} &= 0, \\ (S_1) \quad M_2 L_1^{p-1} + M_1^p - M^p Q_1 &= 0, \\ (S_2) \quad M_1 L_2^{p-1} + M_2^p - M^p Q_2 &= 0. \end{aligned}$$

The invariants N_s can be shown to be integral as follows: Multiplying numerator and denominator of N_s by L_1^s , we get

$$N_s = \frac{M_2^{s+1} L_1^{p-1} + (-1)^s M_1^{p-s} L_1^s L_2^s}{M^p L_1^s}. \quad (1)$$

Multiplying syzygy (S_1) by M_2^s , we have

$$M_2^{s+1} L_1^{p-1} = M^p Q_1 M_2^s - M_1^p M_2^s. \quad (2)$$

* Dickson, *Transactions American Mathematical Society*, Vol. XII, pp. 1-12.

Solving syzygy (S_0) for $L_1 L_2$ and then raising $L_1 L_2$ to the s -th power, we get

$$(L_1 L_2)^s = \sum_{k=0}^s (-1)^k \binom{s}{k} (M^{p+1})^{s-k} (M_1 M_2)^k. \quad (3)$$

Substituting (2) and (3) in (1), we get

$$N_s = \frac{M^p Q_1 M_2^s + (-1)^s M_1^{p-s} \sum_{k=0}^{s-1} (-1)^k \binom{s}{k} (M^{p+1})^{s-k} (M_1 M_2)^k}{M^p L_1^s}.$$

Every term in the numerator of N_s now contains M^p as a factor. Since M^p is prime to L_1^s , the numerator of N_s is divisible by their product, and hence N_s is integral in x_1, y_1, x_2 and y_2 .

Preliminary Theorems.

§ 2. THEOREM. *The sum of the exponents of either set of cogredient variables in any term of an invariant is congruent modulo $p-1$ to the index μ of the invariant.*

This is proved by applying one of the transformations

$$\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix},$$

where a is a primitive root of p .

§ 3. Definition. We shall say that x_1, y_1 form one set of variables and x_2, y_2 the other set.

THEOREM. *The terms of an invariant which are homogeneous in each set of variables form an invariant.*

We write the invariant as a sum of polynomials each homogeneous in each set of variables, and such that the sum of no two of these polynomials has that property. Then, since the linear transformation $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ leaves unchanged the degree in each set of variables, each polynomial is evidently an invariant.

These theorems show that it is sufficient to consider an invariant of the form

$$I = x_2^e \sum_s C_s^{(0)} y_1^e x_1^f + x_2^{e-1} y_2 \sum_s C_s^{(1)} y_1^{e-1} x_1^{f+1} + \dots,$$

where the C 's are integers modulo p , $e = v - s(p-1)$, $f = w + s(p-1)$, s runs from zero to such a value in any sum that none of the exponents in that sum are negative, and $e \equiv f + \mu \pmod{p-1}$.

§ 4. Definition. A semi-invariant is a polynomial I in x_1, y_1 with integral coefficients taken modulo p such that

$$I(x_1, y_1) \equiv b^\mu I(x'_1, y'_1), \quad (\text{mod. } p),$$

for every transformation $\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}$.

We will make considerable use of the semi-invariants y_1 and

$$\lambda = x_1^p - x_1 y_1^{p-1} = \sum_{h=0}^{p-1} \pi(x_1 - h y_1).$$

We have

$$L_1 = y_1 \lambda, \quad Q_1 = \lambda^{p-1} + y_1^{p^2-p}, \\ N_s = x_2^{s^p} \lambda^{p-1-s} + y_2(\quad).$$

Products of the Invariants.

§ 5. *Lemma.* If m and k are any integers for which $1 \leq m \leq p-2$ and $1 \leq k \leq m$, there exists a product $\pi(N)$ of powers of N_1, \dots, N_{p-2} , the first term of whose expansion is $x_2^{mp} \lambda^{k(p-1)-m}$.

If $m = kn$, we may take

$$\pi(N) = N_n^k.$$

If m is not a multiple of k , let n be the integer for which

$$\frac{m}{n+1} < k < \frac{m}{n}.$$

Then we may take

$$\pi(N) = N_n^{(n+1)k-m} N_{n+1}^{m-nk}.$$

§ 6. *Lemma.* There exists a product $\pi(M)$ of powers of M, M_1, M_2 of the form $x_2^u (y_1^v) + \dots$, where u and v are any given integers for which either

$$(1) \quad v = u + k(p-1), \quad (0 \leq k \leq u, \quad v \geq u > 0),$$

or

$$(2) \quad u = v + k(p-1), \quad (0 \leq k \leq v, \quad u \geq v > 0).$$

If (1) holds, we may take

$$\pi(M) = M^l M_1^{k+m} M_2^m, \quad l = u - k - m(p+1).$$

If (2) holds, we may take

$$\pi(M) = M^l M_1^m M_2^{k+m}, \quad l = v - k - m(p+1).$$

Fundamental Theorems.

§ 7. **THEOREM.** Given any invariant $I = \sum_{k=0}^u x_2^{u-k} y_2^k f_k(x_1, y_1)$, determine the integer s such that $s \equiv u \pmod{p}$ and $0 \leq s \leq p-1$. Then $f_t(x_1, y_1)$ has the factor y_1^{s-t} if $t < s$.

The theorem is obvious for $s=0$. If $s \neq 0$, we will apply the transformation $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ to I , and form $I(x+y, y) - I(x, y)$, which must vanish identically. Equating to zero the coefficients of $x_2^{u-k} y_2^k$ ($k=0, \dots, s$), we get the following equations:

$$f_0(x_1 + y_1, y_1) - f_0(x_1, y_1) = 0, \quad (1)$$

$$\sum_{k=0}^{r-1} \binom{s-k}{r-k} f_k(x_1 + y_1, y_1) + f_r(x_1 + y_1, y_1) - f_r(x_1, y_1) = 0, \quad (2)$$

where $\binom{s-k}{r-k} = \frac{(s-k)(s-k-1)\dots(s-r+1)}{(r-k)!}$, $1 \leq r \leq s$, and $\binom{s-k}{r-k} \not\equiv 0 \pmod{p}$ since $s < p$.

The proof is made by mathematical induction. First let us assume that f_0, f_1, \dots, f_m each have the factor y_1 , where $1 \leq m+1 \leq s-1$. Putting for r the value $m+2$ in equations (2), we have

$$\binom{s}{m+2} f_0(x_1 + y_1, y_1) + \dots + \binom{s-m-1}{1} f_{m+1}(x_1 + y_1, y_1) + f_{m+2}(x_1 + y_1, y_1) - f_{m+2}(x_1, y_1) = 0.$$

Putting $y_1 = 0$ gives us $f_{m+1}(x_1, 0) = 0$. Hence, f_{m+1} has the factor y_1 . For $r = 1$, equations (2) give us

$$s f_0(x_1 + y_1, y_1) + f_1(x_1 + y_1, y_1) - f_1(x_1, y_1) = 0.$$

Putting $y_1 = 0$ gives us $f_0(x_1, 0) = 0$, and hence $f_0(x_1, y_1)$ has the factor y_1 . Hence, f_0, f_1, \dots, f_{s-1} each have the factor y_1 .

Let us next assume f_0, f_1, \dots, f_m each have the factor y_1^n ; then we will prove that f_0, f_1, \dots, f_{m-1} each have the factor y_1^{n+1} .

Let $f_t(x_1, y_1) = y_1^n f'_t(x_1, y_1)$, where $0 \leq t \leq m$. From (2) we get, after dividing out y_1^n from the first m equations, m equations of the form of (2) in the preceding discussion, but with f'_t in place of f_t . Hence, $f'_0, f'_1, \dots, f'_{m-1}$ each have the factor y_1 ; and hence f_0, f_1, \dots, f_{m-1} each have the factor y_1^{n+1} .

We have proved that f_0, f_1, \dots, f_{s-1} each have the factor y_1 ; hence f_0, f_1, \dots, f_{s-2} each have the factor y_1^2 . Similarly, f_0, f_1, \dots, f_t each have the factor y_1^{s-t} .

§ 8. *Lemma.* The polynomial f_0 is a semi-invariant. This follows from equation (1) of § 7.

§ 9. *THEOREM.* The highest power of x_1 that occurs in any semi-invariant is congruent to zero modulo p .

As in the theorem of § 2, we can show that the exponents of the same variable in different terms differ by multiples of $p-1$. Hence, let the semi-invariant be

$$f(x_1, y_1) = C_0 x_1^u y_1^v + C_1 x_1^{u-(p-1)} y_1^{v+(p-1)} + \dots$$

Let us suppose that u is not congruent to zero modulo p . Then, since $f(x_1, y_1)$ is unaltered under the transformation $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $f(x_1 + y_1, y_1) - f(x_1, y_1)$ is identically zero. This gives us the equation

$$u C_0 x_1^{u-1} y_1^{v+1} = 0.$$

Since u is not zero, $C_0 = 0$.

Classification of Invariants.

§ 10. *Definition.* An invariant is said to be of type $\{t\}$, if it is of the form $x_2^u f_0(x_1, y_1) + \dots$, where $f_0 \neq 0$, and each (§ 2) exponent of x_1 in f_0 is congruent to t modulo $p-1$, where $1 \leq t \leq p-2$.*

Definition. An invariant is said to be of type $\{0\}$, if it is of the form $x_2^u L_1^r g_0(x_1, y_0) + \dots$, where $g_0 \neq 0$, and each exponent of x_1 in g_0 is congruent to zero modulo $p-1$.

Definition. An invariant is said to be of type $\{0\}'$, if it is of type $\{0\}$ and the exponent of y_1 in $g_0(x_1, y_1)$ is less than $p-1$.†

Definition. An invariant is said to be reduced, if it can be written as the sum of invariants or if its semi-invariant leader can be written as an invariant multiplied by a semi-invariant of lower degree.

Definition. The grade of the semi-invariant of $I = x_2^u L_1^r g_0(x_1, y_1) + \dots$ is the degree of $g_0(x_1, y_1)$.

Reduction of Invariants of Type $\{t\}$.

§ 11. *Lemma.* Any invariant of type $\{t\}$ can be reduced either to an invariant of type $\{0\}$, $\{0\}'$ or to one which contains x_2 as a factor. The grade of the semi-invariant of the reduced invariant is less by $pt+t$.

The general form of such an invariant is

$$I = x_2^a (C_0 y_1^{b+s} x_1^t + \dots + C_m y_1^s x_1^{t+r}) + \dots, \quad (1)$$

where $a = d(p^2 - p) + h(p - 1) + r$, $b = g(p^2 - p) + k(p - 1)$, $r \leq p - 2$, $s \leq p - 2$, $k \leq p - 1$, $h \leq p - 1$ and $1 \leq t \leq p - 2$. The C 's are integers modulo p such that at least one of them does not vanish.

Case 1. $t \leq s$.

Since the semi-invariant leader has the factor x_1^t and y_1^t , it has the factor L_1^t , and hence equation (1) can be written

$$I = x_2^a L_1^t (C_0 y_1^{e+s-t} + \dots) + \dots, \quad (2)$$

where $e = g(p^2 - p) + (k - t)(p - 1)$. This is an invariant of type $\{0\}$, the grade of whose semi-invariant is less by $pt + t$. If $e = 0$, I is of type $\{0\}'$. If $e < 0$, the semi-invariant of equation (2) is identically zero and I has the factor x_2 .

Case 2. $t > s$ and $t - k \not\equiv 0 \pmod{p}$.

Since, in equation (1), $b + t \equiv t - k$ modulo p and this is not congruent to zero modulo p , it follows from § 9 that $C_m = 0$. Hence, as in case 1, the semi-invariant of I has the factor L_1^t and can be reduced to the form of equation (2).

* If an invariant is of the form $I = x_2^u L_1^r g_0(x_1, y_1) + \dots$, where each exponent of x_1 in $g_0(x_1, y_1)$ is congruent to t modulo $p-1$ and $1 \leq t \leq p-2$, it is assumed in the following discussion that $I = x_2^u f_0(x_1, y_1) + \dots$, where $f_0(x_1, y_1) = L_1^r g_0(x_1, y_1)$.

† By § 2, $g_0(x_1, y_1)$ contains only one term which is a power of y_1 .

Case 3. $t > s$ and $t - k \equiv 0 \pmod{p}$.

Since both t and k are less than p , it follows that $t = k$. By § 2, $a + t \equiv b + s \pmod{p-1}$. Hence, $r \equiv s - t \pmod{p-1}$, which gives $r = p - 1 + s - t$. If $C_m = 0$, the reduction is effected as in case 1. If $C_m \neq 0$, there is a condition imposed on h by § 7. Since $a \equiv s - h - t - 1 \pmod{p}$, and since this is less than zero, the semi-invariant of equation (1) must contain y_1 either to the power $p + s - h - t - 1$ or, if this is still negative, to the power $2p + s - h - t - 1$. In the first instance, by § 7, $p + s - h - t - 1 \leq s$. Hence, $h = p - 1 - t + n$, where $0 \leq n \leq s$. The exponent a of equation (1) can now be written in the form

$$[d(p^2 - p)] + [n(p - 1) + s] + [(p - 1 - t)p],$$

and the exponent $b + t$ of equation (1) can be written as

$$p[(g + 1)(p - 1) - (p - 1 - t)].$$

If $g + 1 \leq p - 1 - t$, we will form

$$I' = I - C_m \pi(M) \pi(N) Q_2^d.$$

If $g + 1 = p - 1 - t + l$, where $l > 0$, we will form

$$I' = I - C_m \pi(M) \pi(N) Q_1^l Q_2^d.$$

Here, by § 6, $\pi(M) = x_2^{n(p-1)+s} y_1^s + \dots$. If $s = 0$, we will take $\pi(M) = 1$. By § 5, $\pi(N) = x_2^{(p-1-t)p} \lambda^{(g+1)(p-1)-(p-1-t)} + \dots$. Then the semi-invariant of I' has, as in case 1, the factor L_1^t , and hence has the form of equation (2).

If $g > 0$, I' is of type $\{0\}$ and the grade of the semi-invariant of I' is less than that of I by $pt + t$. Since the term involving the highest power of x_1 in the semi-invariant of I' is of the form $C'_{m-1} y_1^{p^2-p+s-t} x_1^{(g-1)(p^2-p)}$, if $g = 0$, the terms involving x_2^a vanish and I' has the factor x_2 .

In the second instance a similar line of argument shows that $h = 2p - 1 - t + n$, where $0 \leq n \leq s$. This can then be treated like the case above by replacing Q_2^d by Q_2^{d+1} .

Forms of Certain Invariants.

§ 12. *Lemma.* If v is a number of the form $d(p^2 - p) + h(p - 1) + u$, where $0 \leq u < h \leq p - 1$, and if $f(x_1, y_1)$ is a function of x_1 and y_1 which does not contain the factor y_1 , then there is no invariant of the form

$$I = x_2^v \{C_0 y_1^u L_1^r f(x_1, y_1)\} + \dots,$$

unless $r \geq p - h$ or else $C_0 = 0$.

Since L_1 contains y_1 to the first power only, and since $v \equiv p - h + u \pmod{p}$, where $0 < p - h + u \leq p - 1$, f_0 must contain, by § 7, the factor y_1^{p-h+u} ; hence $p - h + u \leq u + r$, and hence $r \geq p - h$.

Remark. If $r < p - h$ and the coefficient of x_2^v is a function of x_1 and y_1 not a constant, then, by § 7, $C_0 = 0$. If the coefficient of x_2^v is a constant, then,

since an invariant in two variables is a special case of a semi-invariant, $C_0 = 0$ by § 9.

§ 13. *Lemma.* If v is a number of the form $d(p^2 - p) + h(p - 1) + u$, where $0 \leq u < h \leq p - 1$, then there is no invariant of either of the forms

$$\begin{aligned} (1) \quad I &= x_2^v (C_0 y_1^u) + \dots, \\ (2) \quad I &= x_2^u (C_0 y_1^v + \dots) + \dots, \end{aligned}$$

where $C_0 \neq 0$.

The first case follows from § 12 by taking $r = 0$ and $f(x_1, y_1) = 1$. If we apply the substitution $(x_1, x_2)(y_1, y_2)$ to the invariant in case (2), we get an invariant of the form of that in case (1). Hence, C_0 in case (2) equals zero.

§ 14. *Lemma.* If the degree u in x_2, y_2 of an invariant is less than p , and if the coefficient of x_2^u is of the form $L_1^r g_0(x_1, y_1)$, where $r > 0$, then g_0 is not zero and the invariant has the factor L_1^r .

Let $I = x_2^u L_1^r g_0(x_1, y_1) + x_2^{u-1} y_2 f_1(x_1, y_1) + \dots$, where $u \leq p - 1$. If g_0 is zero, I has the factor L_2 at least to the first power. This is of degree $p + 1$ in x_2 and y_2 , which is greater than u , and hence I is identically zero.

If g_0 is not zero, then, by § 7, f_0, \dots, f_{u-1} each have the factor y_1 . Since $f_0(y_1, x_1) = f_u(x_1, y_1)$ and since $f_0(x_1, y_1)$ has the factor x_1 , we see that $f_u(x_1, y_1)$ has the factor y_1 . Hence, I has the factor y_1 and hence the factor L_1 . Let

$$I^{(1)} = \frac{I}{L_1} = x_2^u L_1^{r-1} g_0(x_1, y_1) + \dots$$

If $r \geq 2$, $I^{(1)}$ can be shown to have the factor L_1 , and eventually

$$I^{(r)} = \frac{I}{L_1^r} = x_2^u g_0(x_1, y_1) + \dots$$

Hence, I has the factor L_1^r .

§ 15. *Lemma.* There is no invariant of degree less than p in x_2, y_2 whose semi-invariant leader is an invariant of two variables.

Let L_1^r be the highest power of L_1 which is contained in the semi-invariant leader. Then

$$I = x_2^u L_1^r g_0(x_1, y_1) + \dots,$$

where $u < p$ and g_0 is an invariant which does not contain y_1 as a factor. By § 14, I has the factor L_1^r . Hence, let

$$I^{(r)} = \frac{I}{L_1^r} = x_2^u g_0(x_1, y_1) + \dots$$

By § 7, g_0 must contain y_1^u as a factor; hence, $g_0 = 0$. Then, by § 14, I is identically zero.

Reduction of Invariants of Type $\{0\}$.

§ 16. *Lemma.* Any invariant of the form $I = x_2^a (C_0 L_1^r y_1^u) + \dots$, where $a = d(p^2 - p) + h(p - 1) + u$ and $0 \leq u < h \leq p - 1$, can be reduced to an invariant containing x_2 as a factor.

We have shown in § 12 that r must equal or exceed $p - h$.^{*} If $h \geq 2$, the invariant

$$I' = I - C_0 Q_2^d N_{h-1} M^{p-h+u}$$

is an invariant having x_2 as a factor. If $h = 1$ and $d \geq 1$, then $u = 0$ and

$$I' = I - C_0 Q_2^d Q_1 M^{p-1} + C_0 Q_2^{d-1} M^{p^2-1}$$

has the factor x_2 . Here d can not equal zero, since, by § 15, there is no invariant of the form that I becomes if $d = u = 0$ and $h = 1$.

§ 17. *Lemma.* There is no invariant of the form

$$I = x_2^u L_1^r \{C_0 y_1^{b+u} + \dots\} + \dots,$$

where $b = g(p^2 - p) + k(p - 1)$, $0 \leq u < k \leq p - 1$ and $C_0 \neq 0$.

Since $u < p$, then, by § 14, I has the factor L_1^r . Let

$$I^{(r)} = \frac{I}{L_1^r} = x_2^u \{C_0 y_1^{b+u} + \dots\} + \dots$$

Then, by § 13, $C_0 = 0$.

§ 18. *Lemma.* Any invariant of type $\{0\}$ can be reduced either to one of type $\{0\}'$ or to one which contains x_2 as a factor. The grade of the semi-invariant of the reduced invariant is less by $p^2 - 1$.

For the sake of simplicity we will take the general form of an invariant of type $\{0\}$ to be

$$I = x_2^a (C_0 y_1^{b+s} + \dots + C_m y_1^s x_1^b) + \dots, \quad (1)$$

where $a = d(p^2 - p) + h(p - 1) + s$ and $b = g(p^2 - p) + k(p - 1)$. Cases where the argument is different, when all the terms involving x_2^a contain L_1 explicitly as a factor, will be treated separately. It should be noted that a and b have the correct form for all cases, since, by § 2, $a \equiv b + s \pmod{p-1}$ and $a + pr \equiv b + s + r \pmod{p-1}$.

Case 1. $1 \leq k \leq p - 1$.

Since k is not congruent to zero modulo p , it follows from § 9 that $C_m = 0$. Hence, the semi-invariant of any invariant of this form contains y_1 as a factor to the power $s + k(p - 1)$.

If, in equation (1), $a \geq b + s$, let $g(p^2 - p) + k(p - 1) + s = u$, and let $d(p^2 - p) + h(p - 1) + s = u + d'(p^2 - p) + h'(p - 1)$, where $0 \leq h' \leq p - 1$. Since $k \geq 1$, it follows that $u \neq 0$ and $h' \leq u$; hence, there exists a

$$\pi(M) = x_2^{h'(p-1)+u} (C_0 y_1^u) + \dots$$

We will let

$$I' = I - C_0 Q_2^{d'} \pi(M).$$

^{*} It is sufficient to use $r = p - h$. The remaining powers of L_1 can be carried along in the reduction.

If $a < b + s$, let $d(p^2 - p) + h(p - 1) + s = u$ and let $g(p^2 - p) + k(p - 1) + s = u + g'(p^2 - p) + k'(p - 1)$, where $0 \leq k' \leq p - 1$. If $k' > 0$, then, by § 17, $C_0 = 0$. If $k' \leq u$ and $u \neq 0$, there exists a $\pi(M) = x_2^u (C_0 y_1^{k'(p-1)+u}) + \dots$. Then we will let

$$I' = I - C_0 Q_1^{g'} \pi(M).$$

If $u = 0$, I is a function of x_1 and y_1 , and hence a function of L_1 and Q_1 .*

In either case the semi-invariant of I' contains the factors x_1^{p-1} and y_1^{p-1} , unless the semi-invariant of I is zero. Hence, the semi-invariant of I' has the factor L_1^{p-1} , and we have

$$I' = x_2^a L_1^{p-1} (C'_1 y_1^e + \dots) + \dots,$$

where $e = (g - 1)(p^2 - p) + (k - 1)(p - 1) + s$. This is an invariant of type $\{0\}$, the grade of whose semi-invariant is less by $p^2 - 1$. If $g < 1$, I' has the factor x_2 . If $g = 1$ and $k = 1$, I' is of type $\{0\}'$.

Case 2. $k = 0$ and $h \leq s$.

There are four subcases which we will denote by subscripts.

Case 2₁. $h \neq 0$ and $s \neq 0$.

Since $h \leq s$ and $s \neq 0$, there exists a $\pi(M) = x_2^{h(p-1)+s} y_1^s + \dots$. We will first form

$$I' = I - C_m Q_2^d Q_1^g \pi(M) = x_2^a y_1^{s+p^2-p} (C'_0 y_1^{(g-1)(p^2-p)} + \dots) + \dots \quad (2)$$

We see that the semi-invariant of I' has the factor $y_1^{s+p^2-p}$. Since $h < p$, it follows that $h(p - 1) + s < p(p - 1) + s$; and since $h \neq 0$, it follows that $p - h < h(p - 1) + s$. Hence, there exists a $\pi(M) = x_2^{h(p-1)+s} y_1^{s+p^2-p} + \dots$. Let us next form

$$I'' = I' - C'_0 Q_2^d Q_1^{g-1} \pi(M).$$

Then the semi-invariant of I'' has the factors x_1^{p-1} and y_1^{p-1} . Hence, I'' has the factor L_1^{p-1} , and hence

$$I'' = x_1^a L_1^{p-1} y_1^c (C''_1 y_1^e + \dots) + \dots, \quad (3)$$

where $a = d(p^2 - p) + h(p - 1) + s$, $c = s + (p - 1)^2$ and $e = (g - 2)(p^2 - p)$. Then I'' is an invariant of type $\{0\}$, the grade of whose semi-invariant is less by $p^2 - 1$. If $g \leq 1$, I'' has the factor x_2 .

Case 2₂. $h = 0$ and $s = 0$.

By taking the first $\pi(M)$ in case 2₁ equal to unity, we get equation (2). If we next form

$$I'' = I' - C'_0 Q_2^{d-1} Q_1^{g-1} M^{p^2-p},$$

we get equation (3) of case 2₁. If $d = 0$, I is a function of L_1 and Q_1 .* If $g = 0$, I is a function of L_2 and Q_2 .*

* Dickson, *Ibid.*

Case 2₃. $h = 0$, $s \neq 0$ and $d \neq 0$.

The reduction to equation (2) is the same as in the case 2₁. Let

$$I'' = I' - C'_0 Q_2^{d-1} Q_1^{g-1} M^{p^2-p+s};$$

then I'' is in the form of equation (3) of case 2₁. If $g = 0$, I' has the factor x_2 .

Case 2₄. $h = 0$, $s \neq 0$ and $d = 0$.

Let us form

$$I' = I - C_0 Q_1^g M^s.$$

If $g = 0$, I' has the factor x_2 . If $g \neq 0$, the semi-invariant of I' has the factor x_1^s and y_1^s , hence the factor L_1^s . Since the exponent a of x_2 in this case equals s , and this is less than p , then, by § 14, I' itself has the factor L_1^s . If in the beginning

$$I = x_2^s L_1^r g_0(x_1, y_1) + \dots,$$

then I' has the factor L_1^{r+s} . Let

$$I'' = \frac{I'}{L_1^{r+s}} = x_2^s (C_1'' y_1^c x_1^e + \dots + C_m'' x_1^{e+e}) + \dots,$$

where $e = p - 1 - s$ and $c = (g - 1)(p^2 - p) + e(p - 1)$.

From § 7, the semi-invariant of I'' has the factor y_1^s , and hence $C_m'' = 0$. Hence, the semi-invariant of I'' has the factors x_1^e and y_1^e , and hence L_1^e . Since, by § 14, I'' itself has the factor L_1^e , if

$$I''' = \frac{I''}{L_1^e},$$

then I''' is of type $\{0\}$, but the grade of its semi-invariant is less than that of I by $p^2 - 1$. If $g = 0$, I'' has the factor x_2 . If $g = 1$, I''' has the factor x_2 .

Case 3. $k = 0$ and $h > s$.

Since $h > s$, then $d(p^2 - p) + h(p - 1) + s \equiv p - h + s \pmod{p}$, where $0 < p - h + s < p$. By § 7, the semi-invariant of equation (1) has the factor y_1^{p-h+s} ; and since $p - h + s > s$, $C_m = 0$. Hence, if $g \neq 0$, the semi-invariant of I has the factor $y_1^{p^2-p+s}$. If $g = 0$, I has the factor x_2 as a consequence of § 13. Since $h < p$, it follows that $h(p - 1) + s < p^2 - p + s$. Hence, let $u = h(p - 1) + s$. Then $p^2 - p + s = u + (p - h)(p - 1)$. Since $h \neq 0$, it follows that $u \neq 0$ and $p - h < h(p - 1) + s$. Hence, there exists a $\pi(M) = x_2^{h(p-1)+s} y_1^{p^2-p+s} + \dots$. If we form

$$I'' = I - C_0 Q_2^d Q_1^{g-1} \pi(M),$$

then I'' has the form of equation (3) of case 2₁.

It might happen that the semi-invariant of I was of the form $L_1^r g_0(x_1, y_1)$. By § 12, $r \geq p - h$. It is sufficient to use $r = p - h$. If $h > 1$, we will form

$$I' = I - C_m Q_2^d Q_1^g N_{h-1} M^{p-h+s}.$$

If $h = 1$ and $d \neq 0$, we will form

$$I' = I - C_m Q_2^d Q_1^{g+1} M^{p-1} + C_m Q_2^{d-1} Q_1^g M^{p-1}.$$

If $h = 1$ and $d = 0$, then $s = 0$ and

$$I = x_2^{p-1} L_1^r (C_0 y_1^{g(p^2-p)} + \dots + C_m x_1^{g(p^2-p)}) + \dots$$

Since the exponent of x_2 is less than p , then, by § 14, I has the factor L_1^r . Let

$$I' = \frac{I}{L_1^r};$$

then, by § 7, I' has the factor y_1^{p-1} , and hence $C_m = 0$. Thus, in all three cases we have reduced the invariant I to the form where the semi-invariant lacks the highest power of x_1 . This is essentially the form of I at the beginning of this case, and hence the reduction can be completed in the same manner.

In every case we saw that the reduction of an invariant of type $\{0\}$ always led to another invariant of type $\{0\}$. By continuing the reduction, we saw that we could reduce the grade of the semi-invariant each time by $p^2 - 1$, until its grade lay between zero and $p^2 - 1$. Let us suppose the degree of the semi-invariant is then congruent to $s \pmod{p-1}$. Then the exponent of y_1 has the form $n(p-1) + s$, where $0 \leq n \leq p+1$ and $0 \leq s \leq p-2$. This is the case where either $g = 1$ and $k = 1$, or $g = 1$ and $k = 0$, or else $g = 0$. We saw that then I either was or could be reduced to an invariant of type $\{0\}'$, or else it could be reduced to an invariant having the factor x_2 . This proves the lemma of this section.

§ 19. *Lemma.* Any invariant of type $\{0\}'$ can be reduced to an invariant which contains x_2 as a factor.

If I is of the type $\{0\}'$, let us suppose

$$I = x_2^a (C_0 y_1^s) + \dots,$$

where $a = g(p^2 - p) + h(p-1) + s$. If $h \leq s$ and $s \neq 0$, there exists a $\pi(M) = x_2^{h(p-1)+s} y_1^s + \dots$. If $s = 0$, we will take $\pi(M) = 1$. Then

$$I' = I - C_0 Q_2^d \pi(M)$$

has the factor x_2 . If $h > 0$, then either $C_0 = 0$ by § 13, and hence I has the factor x_2 , or else the semi-invariant of I has the form $L_1^r g_0(x_1, y_1)$, where $r \geq p - h$. In this instance, by § 16, I can then be reduced to an invariant having x_2 as a factor.

Reduction of an Invariant in the Degree of x_2 and y_2 .

§ 20. We will let J be a general symbol for an invariant which is expressible in terms of the invariants of § 1. By means of the lemmas of § 11, § 18 and § 19, any invariant can be written as

$$I = J + x_2 () = J + L_2^r I', \quad (\tau \geq 1),$$

where I' is an invariant not divisible by L_2 . If I' involves x_2 , we have similarly

$$I' = J' + L_2^{\tau'} I''.$$

This process can then be repeated, until we get

$$I = J'' + L_2^{\tau''} F(x_1, y_1).$$

Then $F(x_1, y_1)$ is an invariant and hence is a function of L_1 and Q_1 .^{*} This proves the theorem of § 1.

Invariants for Modulo $p = 2$.

§ 21. While there are no invariants of the form N_s for modulo $p = 2$, the reduction just given will hold for this modulus also, if we bear in mind that $s = 0$, and h and k can take only the values zero or unity. Since every invariant modulo 2 is of the type $\{0\}$, and since the lemma of § 16 involves only $h = 1$, the invariants for modulo 2 can be reduced without using the invariants N_s .

Independence of Invariants.

§ 22. THEOREM. *No one of the invariants Q_i, L_i, M_i, M, N_s ($i = 1, 2$; $s = 1, 2, \dots, p - 2$) is a rational integral function of the remaining ones.*

The theorem follows by noting the degrees in x_1, y_1 and in x_2, y_2 , and the following additional facts:

Q_i can not be a function of L_i ($i = 1, 2$). If it were, this function would contain L_i as a factor, and hence Q_i would contain x_i as a factor, which is impossible.

M_i ($i = 1, 2$) can not be a function of M and L_i , for by comparing exponents we can see that M and L_i can occur in such a function only to the first degree, and also that the function can not contain the product $M L_i$. Hence, if such a function exists, it has the form

$$M_i = C_0 M + C_1 L_i.$$

Putting $x_j = y_j = 0$, where $j = 1$ if $i = 2$, and $j = 2$ if $i = 1$, gives $C_1 = 0$. Since M_i is of degree p in y_i and M of degree 1 in y_i , no such function exists.

If $N_s = x_2^{sp} (x_1^{p^2-p-s} + \dots) + \dots$ is a function of the invariants in § 1, such a function can not contain N_t , where $t \neq s$. For if $t > s$, then $tp > sp$, and if $t < s$, $p^2 - p - t > p^2 - p - s$. Furthermore, N_s can not be a function of the invariants L_1, L_2, M, M_1 and M_2 , since these invariants all vanish if $y_1 = y_2 = 0$, and N_s then equals $x_2^{sp} x_1^{p^2-p-s}$.